INCIDENT RESPONSE PROCESS NOTES

(1) The user or server administrator who discovers a potential problem is responsible for immediately investigating the situation or immediately turning that responsibility over to a more appropriate person with confirmation that immediate action will be taken.

(2) Anything out of the ordinary should be investigated.

(3) Investigate without changing any system parameters or log files, and without raising suspicion.

(4) (a) If after no more than one hour of investigation the situation seems to indicate unauthorized access to an HQ system, unauthorized activity on an HQ system, denial of service, non-trivial probing for an extended period of time, or any other activity that could be expected to lead directly to any of the above, then contact the Network Operations Center (NOC), SAIC Operations, SAIC Engineering and SAIC IT Security immediately (any appropriate contact in each Department).

(b) If the situation is commonplace, does not violate policy and is not likely to lead directly to any of the above, then log and share the knowledge as appropriate for purposes of cross-training and the keeping of statistics, but do not treat as a security incident. If the situation is not worth logging, and is therefore below the log threshold, then do not bother to log the situation.

(5) Implement any applicable automatic response actions where defined (these are addressed in separate documentation).

(6) Quickly solicit additional input as appropriate and assist Security in formulating an initial response plan, which will probably be the setting up of a quick meeting to examine the data and establish a more detailed plan (see Step #10 below).

(7) Start a hand-written log of events including dates, times, people contacted, person hours (both contractor and government) and situation details.

(8) Make off-line copies of important system files and of the log (again, without changing any system parameters, log files, and without raising suspicion. It is important to maintain the initial integrity of the log. Spend no more than 30 minutes on this step).

(9) Form an opinion on the impact of letting the current situation persist, on what should be done, and on how quickly it needs to be done.

(10) All involved parties come together to decide how to proceed.

(11) Implement the agreed-upon response plan within 4 hours of the initial suspicion.

(12) Continue to watch the situation and if anything new develops, confer again with the appropriate people (see Step #4(a) above).

(13) See separate documentation regarding response strategies.

(14) NASIRC and NASA IG should be notified if the potential exists for any of the following:

- High public interest
- Public embarrassment
- Occurrence at other NASA Centers
- Degradation of mission readiness
- Extensive denial of service
- High cost of recovery
- Discovery of a major vulnerability
- Large-scale physical damage to IT resources due to human error
- Large-scale physical damage to IT resources due to natural disaster

(15) Submit an ADP/T Security Incident Report form (NHQ 187) to the ITSM. Be sure to include person hours (contractor and government) on the Incident Report form.

Additionally, any incident that involves criminal activity should be reported to NASA IG.